

## Die Sicherheitswarnung beim Zugriff auf das Schulnetz über HTTPS.

Beim Zugriff auf Daten im Schulnetz erscheint ein Sicherheitshinweis mit zwei Warnungen zum Sicherheitszertifikat. Diese Warnungen werden erläutert und es wird ein Weg gezeigt, das Sicherheitszertifikat gültig zu machen. Dies bezieht sich auf Einstellungen am Browser des Benutzers und auf Einstellungen, die am NetWare Server vorgenommen werden müssen.

In den letzten ZPG-Mitteilungen Nr. 29 wurde beschrieben, wie man mit dem Browser oder Explorer auf das Homeverzeichnis im Schulnetz unter der Musterlösung 2 zu Novell Netware zugreifen kann. Beim verschlüsselten Zugriff über HTTPS erscheint dabei folgender Hinweis:

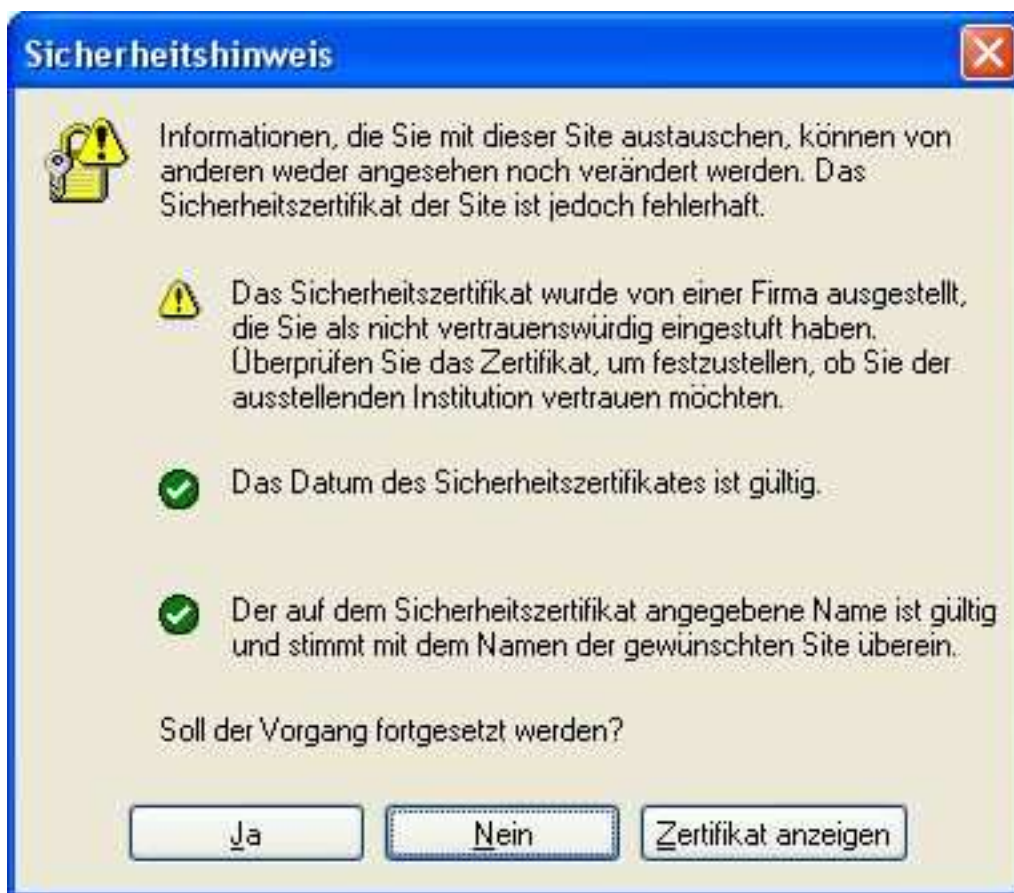


Die untere Hinweis „Der auf dem Sicherheitszertifikat angegebene Name ist ungültig oder stimmt nicht mit dem Namen der Site überein“ ist sehr ärgerlich, soll doch gerade darüber die Identität der Internetadresse garantiert werden. Diese Meldung tritt immer dann auf, wenn die Adresse in der URL und der Name im Zertifikat unterschiedlich sind. Ursache für die Meldung ist, dass in der Musterlösung 2 die angesprochenen Dienste auf der Privaten Karte des GSERVER02 laufen, der Zugriff von außen auf diese Dienste aber über die Public Karte des GSERVER02 bzw. des KSERVER02 erfolgt. Bei der Installation wurde das Zertifikat „SSL CertificateIP-GSERVER02“ für die IP Adresse 10.1.1.22 und das „SSL Certificate DNS-GSERVER02“ für den DNS Namen GSERVER02.netware.ml-bw.de ausgestellt. Deshalb erfolgt beim Aufruf der Adressen von innen auch keine Warnung. Das Feld ist grün. Wichtiger aber ist ein grünes Feld beim Zugriff von außen, denn dort will ich sicher sein, dass ich wirklich mit der angewählten Adresse verbunden bin.

Es gibt einen einfachen Weg, die Situation umzukehren. Die beiden betroffenen Zertifikate müssen erneuert werden. Die Erneuerung von Zertifikaten ist im Zusammenhang mit dem Ablauf des Gültigkeitsdatums von der ZEN Gruppe auf den Seiten des Support Netzes veröffentlicht worden: <http://support-netz.de/dt/nml-letzte-aenderungen.html#zertifikate-m12> .

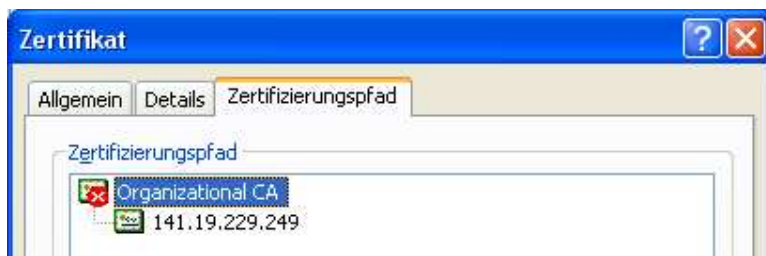
Nach dieser Anleitung kann man die beiden Zertifikate neu erstellen. Diesmal gebe man aber als IP nicht an 10.1.1.22 sondern trage die eigene öffentliche IP ein. Ebenso verfährt man beim DNS Zertifikat, bei dem man den eigenen öffentlichen DNS Namen einträgt. Aber Achtung: Die im Dokument erklärte Prüfung mit PKIDIAG führt jetzt zur „Fehlermeldung“, dass die Namen nicht stimmen. Aber das ist ja gerade so gewollt und schadet weiter nicht.

Dieses Vorgehen ist mit der ZEN-Gruppe und der Hotline abgesprochen. Eventuell wird die ZEN Gruppe zu einem späteren Zeitpunkt ein Verfahren finden, bei dem sowohl von Innen wie Außen alles im grünen Bereich gezeigt wird. Jetzt jedenfalls ist die untere Meldung von innen gelb und von außen grün.



Die obere Warnung hat folgenden Text: „Das Sicherheitszertifikat wurde von einer Firma ausgestellt, die Sie als nicht vertrauenswürdig eingestuft haben. Überprüfen Sie das Zertifikat um festzustellen, ob Sie der ausstellenden Institution vertrauen möchten.“ Die Meldung erscheint, solange das Zertifikat nicht im Browser installiert ist. Dies ist eine Aktion, die jeder an seinem Browser selbst durchführen muss. Die Schritte dazu werden im Folgenden kurz aufgezeigt. Eine ausführlich bebilderte Anleitung liegt als Bildschirmpräsentation bereit unter: <http://lehrerfortbildung-bw.de/netz/muster/novell/material/sogehts/index.html>.

Man wählt in obigen Fenster „Zertifikat anzeigen“. Unter dem Reiter „Allgemein“ sieht man die öffentliche IP seiner Schule mit einem Button „Zertifikat installieren“. Zunächst darf man diesen aber noch nicht den wählen, sondern man muss zunächst unter dem Reiter Zertifizierungspfad die ausgebende Stelle „Organisational CA“ markieren.



Danach wählt man jetzt unter „Allgemein“ den Button „Zertifikat installieren“ aus. Es öffnet sich ein Assistent, bei dem man manuell als Zertifikatsspeicher „Vertrauenswürdige Stammzertifizierungsstellen“ auswählt und „Fertig stellen“. Damit ist das Zertifikat importiert. Glauben Sie nicht, dass nun in Zukunft alles grün ist, denn nun ist kein Sicherheitshinweis mehr notwendig und die Verbindung erfolgt sofort.

*Franz Wrede, Carl-Bosch-Schule Heidelberg*

□